



FIG. 1

"BOB"

"ALICE"

$$\begin{aligned} \sigma &\leftarrow H(x, y, w) \quad \sim 102 \\ s_1, r_1, r_2, r_3, r_4 &\xleftarrow{R} Zq \quad \sim 104 \\ E_1 &\leftarrow (g^{r_1}, (h_1)^{r_1 s_1}) \quad \sim 106 \\ E_2 &\leftarrow (g^{r_2}, (h_1)^{r_2 s_1}) \quad \sim 108 \\ E_3 &\leftarrow (g^{r_3}, (h_1)^{r_3 s_1}) \quad \sim 110 \\ E_4 &\leftarrow (g^{r_4}, (h_1)^{r_4 s_1}) \quad \sim 112 \end{aligned}$$

$$E_1, E_2, E_3, E_4, \langle x, y, w, v \rangle \quad \sim 114$$

$$\Sigma[\Psi, \Gamma] \quad \sim 116$$

$$\sigma \leftarrow H(x, y, w) \quad \sim 118$$

$$s_2, r_5, r'_1, r'_2, r'_3, r'_4 \xleftarrow{R} Zq \quad \sim 120$$

$$E_5 \leftarrow (g^{r_5}, (h_1)^{r_5 s_2}) \quad \sim 122$$

$$x(E_1)^{-(a_2+c_2\sigma)} \times (E_2)^{-(b_2+d_2\sigma)} \times (E_4)^{s_2} \quad \sim 124$$

$$E'_1 \leftarrow (g^{r'_1}, (h_2)^{r'_1 s_2}) \quad \sim 126$$

$$E'_2 \leftarrow (g^{r'_2}, (h_2)^{r'_2 s_2}) \quad \sim 128$$

$$E'_3 \leftarrow (g^{r'_3}, (h_2)^{r'_3 s_2}) \quad \sim 130$$

$$E'_4 \leftarrow (g^{r'_4}, (h_2)^{r'_4 s_2}) \times (E'_1)^{-(a_2+c_2\sigma)} \times (E'_2)^{-(b_2+d_2\sigma)} \quad \sim 132$$

$$\langle E_5, E'_1, E'_2, E'_3, E'_4 \rangle \quad \sim 134$$

$$\Sigma[\Psi', \Gamma'] \quad \sim 136$$

138

$$w' \leftarrow x^{e_1} (v x^{-(a_1+c_1\sigma)})_y^{-(b_1+d_1\sigma)} s_1 \cdot E_5[2] \cdot (E_5[1])^{-\beta_1}$$

$$\text{output } w/w' \quad \sim 140$$

1/2



FIG. 2

